IN THE UNITED STATES

PATENT AND TRADEMARK OFFICE

Applicants:	Harlan Seymour et al.
Application No.:	10/802,646
Filing Date:	March 16, 2004
Title:	Empirical Database Access Adjustment
Examiner:	Alicia M. Lewis
Group Art Unit:	2164
Atty. Dkt. No.:	20423-08590

CERTIFICATE OF ELECTRONIC (EFS-WEB) TRANSMISSION

I hereby certify that this correspondence is being transmitted via the Office electronic filing system in accordance with 37 C.F.R. § 1.8(a)(i)(C) from the **Pacific Time Zone** of the United States on the local date shown below.

Dated: December 5, 2008 By: /Jie Zhang/
Jie Zhang, Reg. No.: 60,242

MAIL STOP APPEAL BRIEF - PATENTS
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

APPEAL BRIEF

Pursuant to the requirements of 37 C.F.R. § 41.37, please consider this document as Appellants' Brief in the present application currently before the Board of Patent Appeals and Interferences (hereinafter "the Board").

I. Real Party in Interest

The subject application is owned by Symantec Corporation of Cupertino, California.

II. Related Appeals and Interferences

There are no known related appeals or interferences that may directly affect, be directly affected by, or have a bearing on the Board's decision in the pending appeal.

III. Status of Claims

Claims 1-6, 8-11, 14, 15, 17-20, and 23-26 stand finally rejected in the Final Office Action dated September 17, 2008 (hereinafter referred to as "Office Action"). Claims 7, 12, 13, 16, 21, 22 are canceled.

The rejection of claims 1-6, 8-11, 14, 15, 17-20, and 23-26 is hereby appealed.

IV. Status of Amendments

All claim amendments submitted to the Examiner during prosecution of the present application have been entered. No amendments were proposed subsequent to issuance of the Office Action. The claims involved in the present appeal are presented in Section VIII of this document.

V. Summary of the Claimed Subject Matter

The claimed invention is generally directed to methods, apparatuses, and computer program products for empirically adjusting authorized accesses to a database based on actual accesses to the database. (See, e.g., Spec. p. 3, lines 11-20, and Figures 1 and 2).

Claim 1: Independent claim 1 is an apparatus for empirically adjusting a user's authorized access to a database 1 (See, e.g., Spec. p. 3, lines 11-20, and Figure 1), the apparatus comprising: coupled to the database 1, a database discovery module 11 configured to determine database structure and the user's authorized access to the database 1 (See, e.g., Spec. p. 4, lines 12-16, p. 6, lines 6-12, p. 7, lines 16-21, and Figures 1 and 2), the user's authorized access including a set of authorized database tables and authorized columns (See, e.g., Spec. p. 6, lines 1-3, and p. 7, lines 16-21); coupled to the database 1, a command monitoring module 12 configured to monitor the user's actual accesses to the database 1 until a preselected quantity of actual accesses have been observed (See, e.g., Spec. p. 6, lines 12-13, p. 10, lines 8-16, p. 11, lines 7-15, and Figures 1 and 2), the user's actual accesses including a set of accessed database tables and accessed columns (See, e.g., Spec. p. 6, lines 1-3, p. 10, lines 8-16, and Figures 1 and 2); and coupled to the database discovery module 11 and to the command monitoring module 12, an analysis module 13 configured to compare the user's actual accesses with the user's authorized access (See, e.g., Spec. p. 13, lines 8-18 and Figure 2) and configured to adjust the user's authorized access taking into account results of the comparing by changing settings within a database access control module 16 to deny the user future database access to an authorized database table or an authorized column that is not in the set of accessed database tables and accessed columns (See, e.g., p. 6, lines 13-17, p. 13, lines 19-24, p. 14, lines 18-22, and Figures 1 and 2).

Claim 5: Independent claim 5 is a computer-implemented method for empirically adjusting a user's authorized access to a database 1 (See, e.g., Spec. p. 3, lines 11-20, and Figure 1), the method comprising the steps of: discovering 21 the user's authorized access to the database 1 (See, e.g., Spec. p. 7, lines 16-21, and Figure 2), the user's authorized access

including a set of authorized database tables and authorized columns (See, e.g., Spec. p. 6, lines 1-3, and p. 7, lines 16-21); observing 22 the user's actual accesses to the database 1 until a preselected quantity of actual accesses have been observed (See, e.g., Spec. p. 10, lines 8-16, p. 11, lines 7-15, and Figure 2), the user's actual accesses including a set of accessed database tables and accessed columns (See, e.g., Spec. p. 6, lines 1-3, p. 10, lines 8-16, and Figures 1 and 2); comparing 23 the user's actual accesses with the user's authorized access (See, e.g., Spec. p. 13, lines 8-18 and Figure 2); and adjusting 24 the user's authorized database access taking into account results of the comparing step by changing settings within a database access control module 16 of a computer-implemented database server to deny the user future database access to an authorized database table or an authorized column that is not in the set of accessed database tables and accessed columns (See, e.g., Spec. p. 13, lines 19-24, p. 14, lines 18-22, and Figures 1 and 2).

Claim 14: Independent claim 14 is a computer-readable medium containing computer program instructions configured to empirically adjust a user's authorized access to a database 1 (See, e.g., Spec. p. 3, lines 11-20, and Figure 1), the computer program instructions performing the steps of: discovering 21 the user's authorized access to the database 1 (See, e.g., Spec. p. 7, lines 16-21, and Figure 2), the user's authorized access including a set of authorized database tables and authorized columns (See, e.g., Spec. p. 6, lines 1-3, and p. 7, lines 16-21); observing 22 the user's actual accesses to the database 1 until a preselected quantity of actual accesses have been observed (See, e.g., Spec. p. 10, lines 8-16, p. 11, lines 7-15, and Figure 2), the user's actual accesses including a set of accessed database tables and accessed columns (See, e.g., Spec. p. 6, lines 1-3, p. 10, lines 8-16, and Figures 1 and 2); comparing 23 the user's actual accesses with the user's authorized access (See, e.g., Spec. p. 13, lines 8-18 and Figure 2); and adjusting 24 the

user's authorized database access taking into account results of the comparing step by changing settings within a database access control module 16 of a computer-implemented database server to deny the user future database access to an authorized database table or an authorized column that is not in the set of accessed database tables and accessed columns (See, e.g., Spec. p. 13, lines 19-24, p. 14, lines 18-22, and Figures 1 and 2).

VI. Grounds of Rejection to be Reviewed on Appeal

The grounds of rejection to be reviewed on appeal are:

(1) whether claims 1-3, 5, 8, 9, 11, 14, 17, 18, 20, and 23-26 were properly rejected under 35 USC § 103(a) as being unpatentable over U.S. Pat. Appl. Pub. No. 2003/0101355 A1 to Mattsson ("Mattsson") in view of U.S. Pat. Appl. Pub. No. 2003/0167229 A1 to Ludwig et al. ("Ludwig");

(2) whether claims 4, 10, and 19 were properly rejected under 35 USC § 103(a) as being unpatentable over Mattsson in view of Ludwig and further in view of an article titled "DIDAFIT: Detecting Intrusions in Databases through Fingerprinting Transactions" by Low, et al. ("Low"); and

(3) whether claims 6 and 15 were properly rejected under 35 USC § 103(a) as being unpatentable over Mattsson in view of Ludwig and further in view of U.S. Pat. Appl. Pub. No. 2005/0097149 A1 to Vaitzblit et al. ("Vaitzblit").

VII. Argument

A. Claims 1-6, 8-11, 14, 15, 17-20, and 23-26 are patentable over Mattsson in view of Ludwig, Low, and Vaitzblit

To render a claim unpatentable under §103, the prior art reference (or references when combined) must suggest or teach *all* the limitations of the claimed invention. *See In re Royka*, 490 F.2d 981 (C.C.P.A. 1974); 35 U.S.C. § 103(a); MPEP §§ 706.02(j), 2143.03. If even a single claim limitation is not taught or suggested by the prior art, then that claim cannot be rejected under §103 over the prior art. *See In re Glass*, 472 F.2d 1388, 1392 (C.C.P.A. 1973). The Examiner's rejection of claims 1-6, 8-11, 14, 15, 17-20, and 23-26 is improper because the suggested combination of Mattsson and Ludwig does not teach or suggest all of the limitations of the rejected claims.

Specifically, independent claim 1 recites:

> ...
>
> coupled to the database, a command monitoring module configured to monitor the user's actual accesses to the database **until a preselected quantity of actual accesses have been observed,** the user's actual accesses including a set of accessed database tables and accessed columns; and
>
> coupled to the database discovery module and to the command monitoring module, an analysis module configured to compare the user's actual accesses with the user's authorized access and configured to **adjust the user's authorized access taking into account results of the comparing by changing settings within a database access control module to deny the user future database access to an authorized database table or an authorized column that is not in the set of accessed database tables and accessed columns.** (emphasis added)

Therefore, claim 1 recites an apparatus that adjusts a user's authorized access by denying the user's future access to database tables and columns that the user was authorized to access but did not actually access. The claimed apparatus is useful, for example, in restricting loosely granted

database access to reduce the possibility of database intrusion. Independent claims 5 and 14 recite similar features.

Neither Mattsson nor Ludwig discloses adjusting "the user's authorized access taking into account results of the comparing by changing settings within a database access control module to deny the user future database access to an authorized database table or an authorized column that is not in the set of accessed database tables and accessed columns" as recited in claim 1. Mattsson discloses a database intrusion detection system that uses item access rates and inference patterns to detect intrusions. See Mattsson, paragraphs [0015] and [0022]. If a user's query activity is within his permitted item access rate, yet his accumulated query results match a relevant inference pattern, then the Mattsson system classifies the related query activity as an intrusion. See Mattsson, paragraph [0044].

The Examiner cited paragraphs 37-39, 42-46, and 52 of Mattsson for disclosure of the adjusting limitation. These paragraphs disclose that the Mattsson system has an intrusion detection module that compares query results with item access rates and inference patterns to detect intrusions, and that if an intrusion is detected then an access control system is alerted and the query results are not transmitted to the requester. The Examiner acknowledged that Mattsson does not disclose denying "the user future database access to an authorized database table or an authorized column that is not in the set of accessed database tables and accessed columns" as claimed. See Office Action, p. 4. The Examiner asserted that this deficiency is remedied by Ludwig.

Ludwig fails to teach or suggest the above cited claim limitation. Ludwig discloses a business platform for payment transactions, and is not related to adjusting user access to databases. See Ludwig, Abstract. The Examiner specifically cited paragraph [0051] of

Ludwig, which discloses methods to verify the identity of a user, including periodically changing passwords and expiring inactive user accounts. Thus, at most Ludwig discloses expiring inactive accounts.

The combination of Mattsson and Ludwig fails to disclose adjusting "the user's authorized access taking into account results of the comparing by changing settings within a database access control module to deny the user future database access to an authorized database table or an authorized column that is not in the set of accessed database tables and accessed columns". As argued above, Mattsson classifies user accesses exceeding permitted item access rate as intrusions, and Ludwig expires user accounts after extended inactiveness. Therefore, if the combination denies the user future database access because of extended inactiveness, as allegedly being taught by Ludwig, such inactiveness would not trigger the authorized access adjustment that takes into account the comparison result, as allegedly being taught by Mattsson, because authorized access adjustments in Mattsson are triggered by query activities that are absent in extended inactiveness. See Mattsson, paragraph [0037]. Therefore, even if Mattsson and Ludwig can arguably be combined, the combination would not disclose or suggest the above-cited claim limitations.

In addition, Ludwig's teaching cannot be combined with Mattsson in a manner that satisfies the other claim elements of claim 1 because the combination would not work. For example, the Ludwig system is totally binary: either an access is observed and the account is left active, or no access is observed and the account is expired. Therefore, the claimed observed "preselected quantity of actually accesses" would have to be zero activity in order for Ludwig to be applicable. But if there is no database access, then no database table or column is actually accessed and there would be nothing for the analysis module to compare.

Similarly, the other references cited by the Examiner against some dependent claims fail to remedy the deficiencies of Mattsson and Ludwig described above. Low discloses a database intrusion detection system that fingerprints SQL statements in order to detect illegitimate accesses. Vaitzblit discloses a database audit system used to monitor, and optionally alert on database activity.

Likewise, the combination of Mattsson, Ludwig, Low, and Vaitzblit also fails to disclose or suggest the claimed features. For example, if Mattsson and Ludwig were combined, at best the combination would provide for monitoring and restricting user's access rates to sensitive data in a database, or monitoring and expiring inactive user accounts. Neither of the two combinations adjusts a user's authorized access by denying the user's future access to database tables and columns that the user was authorized to access but did not actually access. Adding Low and/or Vaitzblit into the combination would not disclose or suggest the claimed features either.

Accordingly, Appellants respectfully submit that a person of ordinary skill in the art would not find the invention of independent claim 1 obvious in view of the cited references. The rejection of independent claims 5 and 14, and of the dependent claims is improper for at least the same reason.

B. Claim 25 is patentable over Mattsson in view of Ludwig

The Examiner's rejection of dependent method claim 25 is improper because the suggested combination of Mattsson and Ludwig does not teach or suggest all of the limitations of claim 25.

Claim 25 depends from claim 5 and recites, inter alia, the following additional claimed feature "generating a map of which tables and columns of the database were accessed during the

observing". This claimed feature at least implicitly recites that some tables and columns were actually accessed during observation, which means that Ludwig cannot be combined with Mattsson in the manner shown in the Office Action in rejecting independent claim 5. See Office Action, pp. 5-6. As argued above, Ludwig expires user accounts after extended inactiveness. If there are actual access to some database tables and columns, Ludwig would not expire the account. As a result, the combination of Mattsson and Ludwig would not teach the following claimed feature "adjusting the user's authorized database access taking into account results of the comparing step by changing settings within a database access control module of a computer-implemented database server to deny the user future database access to an authorized database table or an authorized column that is not in the set of accessed database tables and accessed columns" as recited in claim 5 and incorporated by reference in claim 25. Therefore, Mattsson and Ludwig, whether considered individually or in combination, fail to disclose each and every limitation recited in claim 25.

Accordingly, Appellants respectfully submit that a person of ordinary skill in the art would not find the additional elements of dependent claim 25 obvious in view of the cited references.

C. Claim 26 is patentable over Mattsson in view of Ludwig

The Examiner's rejection of dependent method claim 26 is improper because the suggested combination of Mattsson and Ludwig does not teach or suggest all of the limitations of claim 26.

Claim 26 depends from claim 5 and recites, inter alia, the following additional claimed features:

monitoring the user's actual accesses to the database during an extended period occurring after the preselected quantity of actual accesses have been observed; and

generating an alert in real time regarding the user's actual accesses that are observed during the extended period that were not observed within the preselected quantity of the user's actual accesses.

Neither Mattsson nor Ludwig teaches or suggests the generating limitation. The Examiner cited paragraph [0043] of Mattsson for support of the rejection. Paragraph [0043] of Mattsson is reproduced below in its entirety.

> If the current query result or accumulated record 14 includes a number of rows exceeding a particular item access rate 21, such a request will be classified as an intrusion (step S7), and the access control system 7 will be alerted (step S10).

Paragraph [0043], like the rest of Mattsson is silent as to "the extended period" and "the preselected quantity of the user's actual access" as claimed. The Examiner asserted that "[a]ll accesses observed after the item access rate has been reached, are considered to be observed during the extended period, and not observed within the preselected quantity of accesses." See Office Action, pages 8-9. It appears the Examiner equates the time period after an item access rate has been reached to the claimed "extended period", and equates the database accesses incurred before that to the claimed "preselected quantity of the user's actual access". Appellants submit that in order for the item access rate to be reached, the user much have accessed the item previously. Therefore, under the Examiner's interpretation, the user's actual accesses would have been observed within the preselected quantity of the user's actual accesses, which conflicts to the following claim language "the user's actual accesses … that ***were not*** observed within the preselected quantity of the user's actual accesses" (emphasis added).

Accordingly, Appellants respectfully submit that a person of ordinary skill in the art would not find the additional elements of dependent claim 26 obvious in view of the cited references.

For the foregoing reasons, Appellants submit that the Examiner's rejections of claims 1-6, 8-11, 14, 15, 17-20, and 23-26 were erroneous, and respectfully request reversal.

Respectfully submitted,
HARLAN SEYMOUR ET AL.

Dated: December 5, 2008

By: /Jie Zhang/

Jie Zhang, Attorney of Record
Registration No. 60,242
FENWICK & WEST LLP
801 California Street
Mountain View, CA 94041
Phone: (650) 335-7297
Fax: (650) 938-5200

VIII. Claims Appendix

The claims involved in the instant appeal are as follows:

1. Apparatus for empirically adjusting a user's authorized access to a database, said apparatus comprising:

coupled to the database, a database discovery module configured to determine database structure and the user's authorized access to the database, the user's authorized access including a set of authorized database tables and authorized columns;

coupled to the database, a command monitoring module configured to monitor the user's actual accesses to the database until a preselected quantity of actual accesses have been observed, the user's actual accesses including a set of accessed database tables and accessed columns; and

coupled to the database discovery module and to the command monitoring module, an analysis module configured to compare the user's actual accesses with the user's authorized access and configured to adjust the user's authorized access taking into account results of the comparing by changing settings within a database access control module to deny the user future database access to an authorized database table or an authorized column that is not in the set of accessed database tables and accessed columns.

2. Apparatus of claim 1 further comprising, coupled to the database discovery module and to the analysis module, a storage area configured to accumulate data generated by the command monitoring module.

3. Apparatus of claim 1 wherein the command monitoring module is a sniffer.

4. Apparatus of claim 1 wherein the database is a relational database accessed by a structured query language.

5. A computer-implemented method for empirically adjusting a user's authorized access to a database, said method comprising the steps of:

discovering the user's authorized access to the database, the user's authorized access including a set of authorized database tables and authorized columns;

observing the user's actual accesses to the database until a preselected quantity of actual accesses have been observed, the user's actual accesses including a set of accessed database tables and accessed columns;

comparing the user's actual accesses with the user's authorized access; and

adjusting the user's authorized database access taking into account results of the comparing step by changing settings within a database access control module of a computer-implemented database server to deny the user future database access to an authorized database table or an authorized column that is not in the set of accessed database tables and accessed columns.

6. The method of claim 5 further comprising the step of generating and storing at least one report based upon observing the user's actual accesses to the database.

8. The method of claim 5 wherein the discovering step uncovers any:

tables of the database;

columns of the database;

views of the database;

stored procedures of the database;

user-defined functions of the database; and

triggers of the database.

9. The method of claim 5 wherein the adjusting step further comprises at least one of:

suggesting revised database access control settings to a database administrator;

automatically hardening the database for all times of day;

automatically hardening the database selectively based on time of day;

alerting a database administrator; and

continuing to monitor the user's accesses to the database after conclusion of the observing step.

10. The method of claim 9 wherein the database is automatically hardened using standard SQL commands.

11. The method of claim 9 wherein the database is automatically hardened using database specific application programming interfaces.

14. A computer-readable medium containing computer program instructions configured to empirically adjust a user's authorized access to a database, said computer program instructions performing the steps of:

discovering the user's authorized access to the database, the user's authorized access including a set of authorized database tables and authorized columns;

observing the user's actual accesses to the database until a preselected quantity of actual accesses have been observed, the user's actual accesses including a set of accessed database tables and accessed columns;

comparing the user's actual accesses with the user's authorized access; and

adjusting the user's authorized database access taking into account results of the comparing step by changing settings within a database access control module of a computer-implemented database server to deny the user future database access to an authorized database table or an authorized column that is not in the set of accessed database tables and accessed columns.

15. The computer-readable medium of claim 14 further comprising the step of generating and storing at least one report based upon observing the user's actual accesses to the database.

17. The computer-readable medium of claim 14 wherein the discovering step uncovers any:

tables of the database;

columns of the database;

views of the database;
stored procedures of the database;
user-defined functions of the database; and
triggers of the database.

18. The computer-readable medium of claim 14 wherein the adjusting step further comprises at least one of:
suggesting revised database access control settings to a database administrator;
automatically hardening the database for all times of day;
automatically hardening the database selectively based on time of day;
alerting a database administrator; and
continuing to monitor the user's accesses to the database after conclusion of the observing step.

19. The computer-readable medium of claim 18 wherein the database is automatically hardened using standard SQL commands.

20. The computer-readable medium of claim 18 wherein the database is automatically hardened using database specific application programming interfaces.

23. Apparatus of claim 1, wherein the preselected quantity of actual accesses is sufficiently large that all expected functionalities of applications accessing the database are exercised.

24. The method of claim 5, further comprising:
storing data generated by the observing of the user's actual accesses to the database in a storage area.

25. The method of claim 5, further comprising:
generating a map of which tables and columns of the database were accessed during the observing.

26. The method of claim 5, further comprising:

monitoring the user's actual accesses to the database during an extended period occurring after the preselected quantity of actual accesses have been observed; and

generating an alert in real time regarding the user's actual accesses that are observed during the extended period that were not observed within the preselected quantity of the user's actual accesses.

IX. Evidence Appendix

No evidence of the types described in 37 CFR § 41.37(c)(1)(ix) has been submitted during prosecution of the present application.

X. Related Proceedings Appendix

To the best knowledge of Appellants and Appellants' legal representative, there are no decisions rendered by a court or the Board that may directly affect, be affected by, or have a bearing on the decision of the Board in the instant appeal.